

REMARKS/ARGUMENTS

Examiner asserts that the "Applicant merely recites a plurality of pending applications that contain no relation to the instant invention," Office Action at Page 2. Applicants' maintain that the listed pending applications and issued patents are directed at steganography, and the related technology of digital watermarking, cryptography, content security and management, bandwidth allocation and optimization, and payment systems, and they have been incorporated by reference. Applicant no longer makes any claim of priority.

Rejections under 35 U.S.C. § 112

Claim 13

Applicants respectfully traverse the rejection of claim 13. It is submitted that Claim 13 does further limit Claim 1 because it requires the ADDITIONAL step of scrambling the independent data which is then embedded into the data object, and then the embedded data object is then scrambled. Hence, claim 13 requires two scrambling steps, and is thus proper.

Rejections under 35 U.S.C. § 112

Claims 19 and 20

The examiner says that "the signal quality level" that is referenced in claim 19 is indefinite because there is no previous introduction of the term "signal quality level." It is submitted that the term "the signal quality level" is not indefinite because one of ordinary skill in the art would read the term as referring to the degradation levels of the first level degraded data signal and the second level degraded signal—which are clearly discussed in claim 14. Accordingly, it is requested that this rejection be withdrawn.

With respect to the 112 rejection of claim 20, it is submitted that the term "the predetermined signal quality level" is not indefinite because one of ordinary skill in the art would read the term as referring to the degradation levels of the first level degraded data

Appl. No. 09/731,039
Responsive Amendment dated September 7, 2004
Response to Office Action of April 6, 2004

signal and the second level degraded signal—which are clearly discussed in claim 14.
Accordingly, it is requested that this rejection be withdrawn.

Rejections under 35 U.S.C. § 102

§ 102 Rejections based on Allen

Claims 1-8, 12, 13, 66, and 67 stand rejected as allegedly anticipated by U.S. Patent No. 5,418,713 issued to Allen (hereafter "Allen"). See Page 4 of Office Action.

Claim 1 (and all claims depending therefrom) and Claim 66 (and all claims depending therefrom)

In order for a reference to anticipate a claim, the reference must disclose each and every limitation of the claimed invention, either expressly or inherently, such that a person of ordinary skill in the art could practice the invention without undue experimentation. See *Atlas Powder Co. v. Ireco Inc.*, 190 F.3d 1342, 1347, 51 USPQ2d 1943, 1947 (Fed. Cir. 1999); *In re Paulsen*, 30 F.3d 1475, 1479, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994). Independent Claim 1 recites, *inter alia*, "A method for securing a data object, comprising: providing a data object comprising digital data and file format information; embedding independent data into the data object; and scrambling the data object to degrade the data object to a predetermined signal quality level. The 102 rejection based on Allen is improper for at least the reason that Allen fails to disclose (1) "embedding independent data" and (2) "scrambling the data object to degrade the data object to a predetermined signal quality level" as required by the rejected claims. The 102 rejection is similarly flawed for Claim 66 (and all dependent claims), as Allen does not disclose (1) an "embedder" and (2) a "scrambler" as required by the claim limitations.

Further, regarding Claim 1 and 66, the Examiner asserts that "... Allen teaches a method/system for securing a data object comprising: providing a data object comprising digital data and file format information (fig. 7); embedding independent data into the data object (col. 7, lines 25-33); and [,] scrambling the data object to degrade the object to a predetermined signal quality level (col. 5, lines 58-65)," Office Action at Page 4. The Examiner's assertion is unsupported by Allen. First, Allen does not teach "embedding

independent data" at any point. Instead, Allen appears to disclose an invention for manufacturing duplicates of "original content", not "securing data within the data objects", as per the Applicants' claimed invention. Duplication of "original content" actually teaches away from "embedding", "scrambling", or combinations of the techniques, as per the Applicants' claim language. In fact, Allen discloses in the Abstract [emphasis added]:

The central host server is connected to a communications network for communication to a remote server which controls a manufacturing control device connected thereto. The **manufacturing control device duplicates original content recordings on blank media upon receipt of a data representation of the original content recording from the remote server** which retrieves said data representation for a selected original content recording from the central host server over the communications network.

The Examiner cites Figure 7, as disclosed above, as allegedly having application to Applicant's securing "data objects". However, Figure 7 clearly separates "identification files" (Figure 7, 251) **and** "accounting information files" (Figure 7, 252), from associated content files, including: "reproducible audio file" (Figure 7, 253), "graphics file" (Figure 7, 254), and "full motion video/audio file" (Figure 7, 255) [emphasis added]. This separation teaches away from the Applicants' invention and claim language for at least the reason that Allen teaches duplication of "the original content recording", there is no "embedding of independent data" and no "scrambling". Applicants teach that open access to data objects at degraded "predetermined signal quality level[s]" is likely to induce purchasing of the original data object (which has not been degraded). Allen teaches duplication of "original content", which is not openly accessible, *upon* a consumer purchase.

The Examiner's further assertion that Allen discloses "embedding independent data" is unsupported. Allen teaches, at Col. 7, ll. 25-33 [emphasis added]:

As part of the content capture process, an item data file is created via the item data file formation process 15 that associates these files for each title (in this case an original music recording) and **also includes associated accounting information** (needed to identify all entities to whom any payment of monies is required for reproductions of the reproducible item) **and identification information** (needed to catalog the title for database usage).

There is no teaching of “embedding independent data” nor would it be apparently necessary since Allen associates (e.g., does not embed) identification and accounting with the data, thereby teaching away from Applicants’ claimed invention[s] with **duplication of “original content”**, see Allen at Abstract; Col. 7 ll. 3-5; Col. 11 ll. 21-28; and, Col. 15 ll. 63-68, [emphasis added].

As for Allen’s alleged teaching of “scrambling the data object to degrade the object to a predetermined signal quality level”, Office Action at Page 4, no such method or system is taught. Allen does teach compression. Allen, at Col. 5 ll. 58-65, as the Examiner’s asserts, argues only that: “In order to make the system commercially practical for purposes of transmitting data to remote locations 77 in realistic time periods, the audio data portion of the item of material is mathematically resampled and digitally compressed during the content capture process to reduce its size and thus shorten the overall transmission time of the related item data file over the communications network 50.” But, Allen does not teach “embedding independent data” and “scrambling” “data objects”, let alone “embedding” and “scrambling” of Allen’s disclosed “original content”, at predetermined signal quality levels to entice purchases or otherwise enable various methods for authentication, payment, and allocation of bandwidth as per Applicants’ invention[s]. Allen’s compression is only used “... to reduce ... size and shorten transmission time,” Allen at Col. 6 ll. 14-15. See also, Allen at Col. 8 ll. 3-14; Col. 13 ll. 5-15; and, Col. 13 ll. 38-49.

Because Allen fails to disclose (1) “embedding independent data into a data object” and (2) “scrambling the data object to degrade the data object to a predetermined signal

quality level" as required by Claim 1, the Section 102 rejection of Claim 1 must be withdrawn. Similarly, Allen fails to disclose (1) an "embedder" and (2) a "scrambler" as required by Claim 66. Moreover, for the same reasons that Claim 1 and Claim 66 are patentable over Allen, the claims that depend from Claim 1 and Claim 66 are also patentable. Applicants request the Examiner withdraw the Section 102 rejections of Claims 1 and 66 and all claims depending therefrom based on Allen.

Claims 2, 3, 5 and 6

Applicants respectfully disagree with the Examiner's assertions that "... Allen teaches the step of performing the steps of embedding and scrambling until a predetermined condition is met (col. 7, line 64 through col. 8, line 14)" and "... Allen teaches the predetermined condition comprises reaching a desired signal quality level of the data object (col. 8, lines 3-11)", Office Action at Page 5. Allen teaches compression for the purposes of duplication of the "original content", see above arguments. For the reasons disclosed above, Allen does not teach "embedding" and "scrambling", let alone "... the step of performing the steps of embedding and scrambling until a predetermined condition is met" as required by the claim limitations. The Examiner fails to identify any "predetermined condition" that must be met before any "embedding" and "scrambling" process is stopped. The Examiner has failed to establish a case of anticipation. Applicants therefore request the Examiner to withdraw the Section 102 rejections for Claims 2, 3, 5 and 6 based on Allen.

Claims 4 and 67

Applicants respectfully disagree with the Examiner's assertion that "... Allen teaches the steps of: [d]escrambling the data object to upgrade the data object to a predetermined signal quality level (col. 6, line 61 through col. 7, line 5); and [d]ecoding the embedded independent data (col. 11, lines 21-28)", Office Action at Page 5, it is illogical to assert that Allen teaches "descrambling" and "decoding embedded independent data" since Allen does not teach "embedding" and "scrambling" in the first place. Additionally, Allen at Col. 6 ll. 61

through Col. 7 ll. 5, is a reiteration of “manufacturing” Allen’s “original content” upon “duplication”. Allen, at Col. 11 ll. 24-26, teaches away from the Applicants’ invention[s] disclosing [emphasis added]: “[t]he royalty accounting 32 is updated **upon duplication of an original content** recording at the remote location”. That Allen is directed at “duplication of an original content recording” is antithetical to the teaching of “embedding” and “scrambling” to assist with enticing consumers to buy after listening or viewing content in an “embedded” and “scrambled” state. This initial purchase is made after listening or viewing a degraded signal and thus not the “original content” of Allen. Nor, is any mention of “embedding” provided in Allen to assist with determination of consumer demand, authentication, payment, and bandwidth allocation as argued by the Applicants. Applicants therefore request the Examiner to withdraw the Section 102 rejections for Claims 4 and 67.

Claim 13

Applicants respectfully disagree with the Examiner’s assertion that “... Allen teaches the step of scrambling the independent data before the embedding step so that the embedding step embeds the scrambled independent data into the data object (col. 7, lines 25-33)” Office Action at Page 6. As argued previously, Allen apparently teaches associating “accounting information” and “identification information”, Allen at Col. 7 ll. 25-33, with his “original content.” Associating accounting or identification information with the “original content” is not equivalent with “embedding independent data” into the “original content”. Moreover, Allen does not teach “scrambling” of any “independent data” prior to an encoding step. No “embedding” or “scrambling” is disclosed. Claim 13 requires “scrambling the independent data before the embedding step so that the embedding step embeds the scrambled independent data into the data object.” Applicants therefore request the Examiner to withdraw the Section 102 rejection for Claim 13.

§ 102 Rejections based on Harada et al.

Claims 60 and 63-65 stand rejected as allegedly anticipated by U.S. Patent No. 6,687,683 issued to Harada et al. (hereafter “Harada et al.”). See Page 6 of Office Action.

Claim 60 (and all claims depending therefrom)

Applicants respectfully disagree with the Examiner's assertion that " Harada et al. teaches a method for bandwidth allocation, comprising: Presenting a plurality of data objects to a user, each data object having a security application (fig. 2, ref. Num 130 and 140); Linking at least a first data object to at least a second data object (col. 8, lines 33-43); Wherein a characteristic of the first data object causes a change in the second data object (col. 25, lines 54-64)," Office Action at Page 6. First, Harada et al. apparently teaches: "[A] data protection system obtains data having a first content on which a first encryption has been performed and a second content on which a second encryption has been performed, the second encryption more difficult to break than the first encryption," Harada et al. at Abstract. There is no apparent linking between the two contents-- each is separately encrypted by a different encryption process. It is unclear to the Applicants how this relates to bandwidth allocation based on presenting two linked data objects wherein a characteristic of the first data object causes a change in the second data object. Harada et al. teaches away from such linking apparently teaching that no access is offered to his " encrypted content".

Examiner's cites of Figure 2 confirms that there is no direct link between the separately encrypted contents. Harada et al. at Col. 8 ll. 33-41 similarly discloses that the two contents are separate and stored for different purposes:

There are two types of music content, i.e., a music content for sample with a lower quality that has been sampled at a 16-KHz sampling rate and a music content for sale with a higher quality that has been sampled at a 64-KHz sampling rate. In this specification, the former one is called a "C1 content" and the latter one is called a "C2 content". An encrypted C1 content 130 is the C1 content that has been encrypted, and an encrypted C2 content 140 is the C2 content that has been encrypted.

If the two contents are separately encrypted it is not possible to meet the claim limitation “wherein a characteristic of the first data object causes a change in the second data object”. The cited claim language of Harada et al., at Col. 25 ll. 54-64, does not cure this deficiency:

[S]econd content decryption means for decrypting the second content using a second decryption method that corresponds to the second encryption and is more difficult than the first decryption method when the data that has been obtained by the obtaining means includes the second content

Encryption is directed at data securing it for transport. Upon decryption, the data is “in the clear”. That Harada et al. is teaching storing content at different quality levels, his C1 and C2, separately and with separate encryption functions means that more bandwidth will be used as each object will be stored twice. This logically assists with determining what content is to be made accessible but does not result in “linking at least a first data object to at least one second data object” as required by the claim. Further, as Harada et al. argue at Col. 3 ll. 10-13 [emphasis added], “[f]urthermore, different encryption is used for the distribution and the recording of second contents, so that even if an encryption algorithm is decrypted, another one is **not influenced**.” The result is that it would undermine Harada et al.’s supposed security system if there were “linking” as per the Applicants’ claim limitations. Applicants therefore request the Examiner to withdraw the Section 102 rejection for Claim 60 and all claims that depend therefrom.

Claim 63

Applicants respectfully disagree with the Examiner’s assertion that “ ... Harada et al. teaches a signal quality level of the second data object is increased with the predetermined key (fig. 6, ref. num S312)” Office Action at Page 6. As argued previously, there is no linking between the first and second “contents” of Harada et al. Harada et al. emphasizes the separation of content at different quality levels for “Trial” or “Recording”, Harada et al. at

Figure 6. A user who decides to buy "C2" may never have seen or heard "C1" nor would it logically follow that these scenarios relate to the claim limitation "wherein a signal quality level of the second data object is increased with a predetermined key." The C2 content is stored at a *fixed* signal quality level and is decrypted from its encrypted state, no predetermined key is associated with increasing signal quality since Harada et al.'s keys are strictly for encryption and decryption and thus have no association with the signal's quality or any level that may be changed by a predetermined key, as taught by the Applicants. Applicants therefore request the Examiner to withdraw the Section 102 rejection for Claim 63.

Claim 64

Applicants respectfully disagree with the Examiner's assertion that "... Harada et al. teaches the predetermined key comprises at least one session key (col. 15, lines 1-5)," Office Action at Page 6. Harada et al. discloses encryption keys, not predetermined keys which have the functionality of the claim limitation in Claim 63 (from which Claim 64 depends) "a signal quality level of the second data object is increased with a predetermined key". The "disk key encryption unit 1220 encrypts the created disk key using each of a plurality of master keys 1219" Harada et al. at Col. 15 ll.1-2 is not equivalent with "session keys" as taught in the art. The claim limitation "the predetermined key comprises at least one session key" is not logically met since the alleged second "content" of Harada et al. is encrypted, preventing access to the "content" and performed without regards to linking between the first and second data objects, as argued previously in connection with Claim 60. Applicants therefore request the Examiner to withdraw the Section 102 rejection for Claim 64.

Claim 65

Applicants respectfully disagree with the Examiner's assertion that "... Harada et al. teaches at least one session key adjusts a payment for the second data object (col. 15, lines 6-14)," Office Action at Page 7. Harada et al. apparently disclose decryption and then

re-encryption of C2 content. This teaches away from enabling "session keys" as described by the Applicants to assist with adjustments in pricing and allocation of bandwidth as each C2 content apparently is encrypted, decrypted and re-encrypted, after payment has been made, Figure 7. Harada et al.'s "content" is never "open" to users who may decide to increase the bandwidth for linked first and second data objects, where the payment information is "at least one session key adjusts a payment for the second data object" as per the claim limitation. That a chain of encryption leaves the content inaccessible makes use of session keys illogical, as payment is made prior to C2 content being transferred to the user and the content is still encrypted, Harada et al. at Figure 6 and 7. Harada et al. does not disclose any session keys much less a session key that adjusts a payment for the second data object. Applicants therefore request the Examiner to withdraw the Section 102 rejection for Claim 65.

Rejections under 35 U.S.C. § 103

In order to "establish a *prima facie* case of obviousness, three basic criteria must be met." MPEP § 7.06.02(j). First, there must be some motivation or suggestion to modify the reference or to make the proposed combination. Second, there must be a reasonable expectation of success. "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the applicant's disclosure." MPEP § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). Third, the combined references must teach or suggest all claim limitations.

The Examiner has failed to establish a *prima facie* case of obviousness to the extent that there is no motivation or suggestion to make the proposed combinations of the references as directed by the Examiner. According to the MPEP,

[i]n order to support a conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner *must present a convincing line of reasoning* as to why

the artisan would have found the claimed invention obvious in light of the teachings of the references.

MPEP 2142 (citing *Ex parte Clapp*, 277 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)) [emphasis added]. Further, “[w]hen the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the examiner to explain why the combination of teachings is proper.” MPEP 2142 (citing *Ex Parte Skinner*, 2 USPQ2d 1788 (Bd. Pat. App. & Inter. 1998)).

The Federal Circuit has recently emphasized the importance of providing evidence of motivation to combine in *Winner Int’l Royalty Corp. v. Ching-Rong Wang*, 202 F. 3d 1340, 1348-49 (Fed. Cir. Jan. 27, 2000). “Although a reference need not expressly teach that the disclosure contained therein should be combined with another . . . the showing of combinability, in whatever form, must nevertheless be ‘**clear and particular**.’” *Winner*, 202 F. 3d at 1348-49 (citations omitted). Further, the “absence of such a suggestion to combine is *dispositive* in an obviousness determination.” *Gambro Lundia AB v. Baxter Healthcare Corp.*, 11 F.3d 1573, 1579 (Fed. Cir. 1997) [emphasis added].

Applicants submit that the Examiner has not satisfied his initial burden of providing “clear and particular” evidence of motivation to combine for any of the proposed combinations of references. More significantly, the references, even in combination, do not disclose all elements of the Applicants’ claimed invention[s].

§ 103 Rejections based on Allen further in view of Wasilewski et al.

Claims 9-11 and 21-48 has been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Allen (U.S. Patent No. 5,418,713) in view of Wasilewski et al. (U.S. Patent No. 5,870,474). Examiner asserts that “... Allen teaches all the limitations of claim 1, above,” Office Action at Page 7. This assertion is unsupported. Allen as disclosed earlier teaches “duplication” of “original content” for the reasons discussed above. This teaches away from the present invention. Also, as discussed above, Allen neither mentions nor discloses any form of “embedding” or “scrambling”.

First, the combination fails to disclose all of the elements of independent Claims 1, 21, and 31 and all claims that depend therefrom. That neither reference mentions “embedding”, “encoding independent authentication data into the data object”, or scrambling based on transfer functions, the references cannot yield the claimed inventions of the Applicants even in combination. The Applicants Specification discusses limitations to proposed “copy protection” schemes, including blanket application of encryption, digital rights management, and the like, to the distribution of the content. Wasilewski et al. describes “conditional access” not “open access” in any form. Asserting that Allen includes “copy protection” is illogical in the context of his disclosure since he emphasizes “duplication” not “protection” of content. Nonetheless, the combination of the two does not disclose all of the elements of the claimed invention[s].

Second, it is unclear that the Examiner’s reliance on assertions that “some form of copy protection would be desirable” relates to the Applicants’ claimed inventions of providing open access to data objects. Applicants maintain that copying of “data objects” will happen. By offering accessible data objects that are scrambled with transfer functions at predetermined signal quality levels, unlike the teachings of Wasilewski et al. to *restrict* access, choices over how much improved quality (even quantity) can be made by the consumer. As the signal quality improves, more embedded independent data is recovered. The property of robustness taught by the Applicants refers specifically to resistance against signal manipulations, contrary to the Examiner’s own definition. Thus, the Applicants respectfully request further explanations/support (for example, other citations or an affidavit if based on personal knowledge) for the Examiner’s assertions that a “robust open watermark” has the following properties: “easy to be seen by any person wishing to access the data”; “robust, the person will find it very difficult to remove the watermarking feature if the person were to choose to cheat the copyright holder”; and, “[t]he combination of a robust open watermark provides an easy to acknowledge, but very difficult to break, method of protecting copy written data”, Office Action at Page 8 and 10. It is unclear to the Applicants where these assertions originate, as they do not appear to be correctly supported in the art or by the Applicants Specification or claims. There are trade-offs between robustness, signal quality, and security in digital watermarking schemes in the art,

and the Examiner appears to contradict these trade-offs. For at least these reasons the Section 103 rejections should be withdrawn.

Claim 21

The Applicants respectfully disagree with the Examiner's assertions that Allen in combination with Wasilewski et al. anticipates Claim 21 and the claims that depend therefrom. The Examiner incorrectly asserts that Allen's method comprises: "... [p]roviding a data object comprising digital data and file format information (fig. 7); and, manipulating the file format information based on at least one signal characteristic of the data object (col. 5, lines 58-65)," Office Action at Page 9. Figure 7 does not disclose digital data and file format information that can be "manipulated" as per the claim limitation. Allen, at Col. 5 ll. 61-63, discloses that the "original content" may be "... mathematically resampled and digitally compressed during content capture..." *not* "encoding independent authentication data into the data object" and "manipulating the file format information based on at least one signal characteristic of the data object", as required by the claim, prior to "distributing a data object". Because Wasilewski et al. teaches conditional access by "encapsulating" content in encryption, "manipulating the file format information based on at least one signal characteristic of the data object", is *not* possible. Figure 3 explicitly recites three layers of encryption preventing access to the data object, teaching away from the claimed invention, Wasilewski et al. at Col. 7 l. 64 – Col. 8 l. 7:

FIG. 3 presents a functional diagram of the presently preferred conditional access model. The present invention provides three functional levels of protection: (1) program encryption, (2) control word encryption and authentication, and (3) entitlement message encryption and authentication. At the first level, the program bearing MPEG-2 transport packets are encrypted using random number generated keys, referred to hereinafter as control words. At the second level, the control words are encrypted using a second randomly generated key. This

second key is referred to hereinafter as a multi-session key (MSK). At the third level, the multi-session key is encrypted using a public key cryptography technique.

The Applicants' invention offers improvements over handling content by providing *open access* while including data object specific tracking, authentication, payment, and bandwidth allocation based on the step of "encoding independent authentication data". As previously argued, Allen, in combination with Wasilewski et al., does not yield the elements of the claimed invention; thus, the 103 rejection must be withdrawn.

Claim 31

The Applicants respectfully disagree with the Examiner's assertions that Allen in combination with Wasilewski et al. anticipates Claim 31 and the claims that depend therefrom. The conditional access schemes of Wasilewski et al. depend on the devices not the "data objects" for enabling access. Wasilewski et al. does not allow "(1) embedding independent data into a data object; (2) scrambling the data object; (3) distributing the scrambled data object; (4) distributing at least one predetermined key that enables access to the data object; and, (5) descrambling the scrambled data object with the predetermined key". Wasilewski et al. at Figure 3 discloses that what is distributed is "MPEG-2 WITH CONDITIONAL ACCESS", Wasilewski et al. Figure 3 ref. 152. The three levels of encryption in Figure 3 rely on a third party authority, what is called a "conditional access authority" by Wasilewski et al. at Col. 22 ll. 49-60:

Each STU 90 has a public key/private key pair. The private key is secured within the STU 90 in a secure processor. The associated public key is then published in a public key database server maintained by a conditional access authority 400. When an SP 110 wishes to provide conditional access to its programming for a particular STU 90, the CAM 30 looks up the public key for the STU 90 and sends the MSK to the STU 90 encrypted with the public

key of that STU 90. The STU 90 can then decrypt the MSK using its corresponding private key. The CAM 30 maintains a data base of valid STU 90 public keys, which it periodically updates from the conditional access authority 400.

Wasilewski et al. thus teaches away from “descrambling the scrambled data object with the predetermined key” to improve signal quality and determine how the recovered, embedded “independent data” is utilized, relying instead on a “conditional access authority”. Wasilewski et al.’s “public key/private key pair” is specific to the “STU” (set-top box), not the “data object” of the Applicants. For arguments sake, Wasilewski et al. would need one STU per “data object” to make each object unique, but would still not present the programming in predetermined signal quality levels, for a given data object, that are embedded with independent data so that a consumer was able to “click through” to higher predetermined signal quality levels. Claim 31’s dependent claims are directed at these novel features. Encryption and traditional digital signatures, as is known in the art and taught by Wasilewski et al., can easily be stripped from programming content without any price paid on the quality of the content. Digital watermarking is directed at causing signal degradation when attempts are made at erasure of the embedded data as well as causing nonauthentication of the embedded signal. Wasilewski et al. could not prevent differencing of “encrypted” with “decrypted” “programming” by the consumer to construct a set-top box (i.e., the decrypted data is in the clear at the consumer’s set-top box). The Applicants’ invention would not suffer such systemic attacks since the data objects are individually prepared by “embedding” and “scrambling”, as argued previously. The benefits of “descrambling the scrambled data object with the predetermined key”, a required claim element of Claim 31, enables authentication, payment measurement, measurements of bandwidth allocation and signal quality parameters. Allen or Wasilewski et al., even in combination, clearly fail to disclose all of the claim elements. For these additional reasons the Section 103 rejections must be withdrawn from Claim 31 and the claims that depend therefrom.

§ 103 Rejections based on Harada et al. further in view of Allen

Claims 14-20, 49-54, 57-59, 61 and 68 has been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Harada et al. (U.S. Patent No. 6,687,683) in view of Allen (U.S. Patent No. 5,418,713). Examiner asserts that “ ... [I]t would have been obvious to combine providing a data signal comprising digital data and file format information, as taught by Allen, to the method of Harada et al. because the file format information tells the system what types of data are contained in the file, thereby allowing the system to determine which methods would best be utilized,” Office Action at Page 17. This assertion is unsupported. Harada et al. apparently teach that two contents can be stored in two separate locations. Two separate encryption methods for each of the stored contents are applied making either stored content completely inaccessible—they are stored in an encrypted state. Additionally, they are not prepared in such a manner, as per teachings of the Applicants, as to enable signal quality improvement over a single data object. Significantly, Harada et al. also apparently teaches that content is re-encrypted when recorded. In fact, when copying or “recording” is permitted for “C2 content”, it is re-encrypted on the media, specifically a memory card, see Harada et al. at Figure 6 & Figure 7; Col. 13 ll. 29-34; Col. 15 ll. 13-14; Col. 20 ll. 61-64; and, Col. 22 ll. 22-28. Combining Harada et al. with Allen fails to disclose the claim elements of independent Claims 49 and 68 and all claims that depend therefrom. As argued previously, Allen neither mentions nor discloses any form of “embedding” or “scrambling”. Allen, as disclosed earlier, teaches “duplication” of “original content.” This teaches away from the present invention. That the content of Harada et al. is encrypted, it would not be possible to combine Allen’s duplication since the signal would be inaccessible as an inherent property of encryption. For at least this reason, the rejection of claim 14 (and the claims that depend therefrom) should be withdrawn.

Second, the combination of Harada et al. with Allen fails to disclose the claim limitations of 49 and 68. Harada et al., teaches a means of creating 2 different quality settings for 2 different access scenarios, Harada et al. at Figure 6 & 7. The content for

either scenario is encrypted and is re-encrypted when stored onto media, as discussed above. That being said, it would not be possible to “apply a steganographic technique for embedding independent data into the data signal”, as required by independent claim 49, since the data signal is encrypted. As applied to claim 68, Harada et al.’s encryption would prevent a “first selector” and thus any subsequent “second selector” to scramble a *single data signal* to different degraded quality levels. Harada et al. relies on content being separately stored in an encrypted state, neither data signal *is accessible* even after recording to a media, so it is illogical to conclude that one, let alone two or more scrambling states for a single data signal would be openly accessible. The Applicants’ claimed inventions represent improvements over managing access to the contents of Harada et al., Allen or combinations of both, by enabling consumers to determine the level of quality and making measurements of the data object more discrete based on manipulations of the data objects’ signal characteristics or payment thresholds that can be associated with such signal manipulations, as presented in the dependent claims. Harada et al, Allen, even in combination fail to disclose all of the claim elements. For at least these reasons, Section 103 rejections must be withdrawn from Claims 49 and 68 and the claims that depend therefrom

§ 103 Rejections based on a combination of Harada et al. and Allen further in view of Ichien et al.

Claims 55 and 56 has been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Harada et al. (U.S. Patent No. 6,687,683) in view of Allen (U.S. Patent No. 5,418,713), and in further view of Ichien et al. (U.S. Patent No. 6,373,892). Examiner asserts that “Ichien et al. teaches the predetermined key is based on a signal quality threshold that is adjustable in at least one of a time, a frequency, a bit depth, and measurement of payment that may be adjusted fro at least one of a time, a frequency, and a bit depth (col. 6, lines 34-51),” Office Action at Page 23. Applicants respectfully disagree. First, combining Ichien et al.’s “key” fails to disclose the elements of the claims. In fact, there is no apparent relationship with the “keys” of the Applicants. Ichien et al. at Abstract: “

[a]t the time of coding a video signal, conversion is carried out for make large a distance between an ordinary digitized video signal and a key signal indicative of whether an image indicates background or foreground for data compression.” Arguments regarding Harada et al. and Allen in combination have been made above. Adding Ichien et al. does not cure the lack of missing claim elements in Claims 55 and 56, instead strictly determining whether an “...image indicates a background or foreground...” as argued above.

Second, where is the motivation to combine Harada et al. and Allen with Ichien et al.? Ichien et al.’s “key” is not derived from the signal after *first* embedding and scrambling said signal, as required by Claim 55 (depending from Claim 49), nor does it effect “a measure of payment”, as required by Claim 56 (depending from Claim 49). It is not derived from said embedded and scrambled signal, as required by Claim 49, from which 55 and 56 depend. Deciding whether an image should be in the foreground or background of a video signal has no relationship to the claim limitations including: “the predetermined key is based on a signal quality threshold that is adjustable in at least one of a time, a frequency, and a bit depth” and “the predetermined key is based on a signal quality threshold that is adjustable in at least of one of a time, a frequency, a bit depth, and a measure of payment that may be adjusted for at least one of a time, a frequency, and a bit depth”. For these reasons, the Section 103 rejections must be withdrawn.

§ 103 Rejections based on Harada et al.

Claim 62 has been rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Harada et al. (U.S. Patent No. 6,687,683). Examiner asserts “Harada et al. teaches an increased quantity of the first data object causes a signal quality level of the second data object to increase (col. 14 lines 9-46, the Examiner treats the increased quantity of the first data object as an increased amount of money for the first data object will cause the signal quality of the second data object, the full audio file, to increase), Office Action at Page 24. Applicants respectfully disagree. The 2 sets of contents of Harada et al. are stored in separate “capsules” as well as being encrypted by different methods, as argued above, and therefore *cannot* be linked. Harada et al. at Col. 14 ll. 24-29 teaches

away from Claim 62, and fails to disclose all of the claim elements, stating: "... when detecting that the user has selected to purchase ... the controller 1120 instructs the second content processor 1210 in the memory card writer 1200 to replay the C2 content 40." Harada et al. does not teach linking between his C1 and C2 content and thus it is not possible for the required claim limitation to be fully met, namely: "an increased quantity of the first data object causes a signal quality level of the second data object to increase".

Second, Applicants disagree with the Examiner's treatment that the first data object is "an increased amount of money for the first data object" as Harada et al. does not teach that his first data object, allegedly the C1 content, can be "increased in quantity" *causing* a "signal quality of the second data object to increase". The C1 and C2 contents are separately stored and encrypted separately, as argued previously. That consumers may listen to C1 content as a "trial version" it is unclear how the Examiner can interpret that to mean there is an increased quantity of C1 content affecting the quality of the C2 content—the stored contents do not effect each other nor are they changed by actions on either the first or second contents. The claimed invention requires such linking, as does Claim 60 from which this claim depends. For these reasons, the Section 103 rejections must be withdrawn.

Conclusion

Applicant maintains that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that an interview with Applicant's representative, either by telephone or in person, would further prosecution of this application, we would welcome the opportunity for such an interview.

It is believed that no other fees are required to ensure entry and consideration of this response.

Respectfully submitted,

Date: September 7, 2004

By:



Scott A. Moskowitz